Privacy Regulation in the U.S.

A Practical Guidance® Practice Note by Kirk Nahra, Arianna Evers, Ali Jessani, Genesis Ruano, and Samuel Kane, WilmerHale

Kirk Nahra
WilmerHale

Arianna Evers
WilmerHale

Ali Jessani
WilmerHale

Genesis Ruano
WilmerHale

Samuel Kane
WilmerHale

This practice note is intended to give privacy officers and other privacy professionals an overview of how commercial privacy issues are regulated in the United States. While this chapter is not intended to be exhaustive in terms of all potentially applicable U.S. privacy laws, it should provide privacy professionals with a general foundation on these issues and a starting point on how to evaluate data privacy compliance obligations for their organizations.

As we elaborate on below, the U.S. generally regulates privacy through four main approaches: sector-specific laws, use case-specific laws, laws applicable to certain types of data (data-specific laws), and comprehensive privacy laws (at the state level). We have used this framework to summarize the laws, regulations, and issues that privacy professionals are most likely to come across in their work.

Recent trends in U.S. privacy law can help privacy professionals understand where the law may be going. While change in U.S. privacy law at the federal level continues to remain a possibility, state legislatures continue to be at the forefront of new privacy regulations. Iowa, Tennessee, Indiana, Texas, Oregon, Delaware, and Montana have joined early adopters of comprehensive privacy laws (California, Virginia, Colorado, Utah, and Connecticut) as of 2023. In addition to comprehensive state privacy laws, many states have also passed sector, industry, and data-specific laws as states race to replicate successful statutes and address data issues that have emerged in the wake of the COVID-19-driven shift towards remote work and school. As a result, there has been a strong recent focus on data brokers and more "sensitive" categories of data, such as health information and genetic data. Regulators have increased attention on issues relating to Adtech and targeted advertising more generally, and many of the laws

and regulatory trends discussed in this practice note are driven by that focus.

While many of these statutes share similar principles—indeed, newer bills frequently draw inspiration from the text and implementation issues of prior statutes—they vary in definitions, scope, and enforcement rights. The complexity created by this web of statutes has been further magnified by the creation of nontraditional privacy obligations and the cross-industry "digital transformation" that occurred in the wake of COVID-19. In this developing privacy landscape, more companies risk failing to understand the scope of their privacy compliance obligations. Companies which handle "sensitive" information or engage in practices that would constitute a heightened risk, such as automated decision-making, should be particularly on guard as many state laws devote particular attention to those use cases and definitions can vary by state.

Notably, companies and privacy professionals must consider the abundance of laws that implicate privacy considerations, such as information security laws, laws that regulate government data use, additional data-specific laws like those governing health status, among others, which are not covered in this note. In addition, not all of these laws will be applicable to every company.

For related guidance, see California Consumer Privacy Resource Kit (CCPA and CPRA), First-Year Associate Resource Kit: Data Security and Privacy, Generative Artificial Intelligence (AI) Resource Kit, HIPAA Resource Kit, and Summer Associate Resource Kit: Data Security and Privacy.

For related trackers, see Privacy Legislation Tracker: State Comprehensive Consumer Privacy Bills (2024) and Biometric Privacy State Legislation Tracker (2023-2024); Federal Trade Commission (FTC) Consumer Privacy Enforcement Tracker, and HIPAA Regulatory Enforcement Tracker.

Sector-Specific Privacy Laws

Privacy laws at the federal level have primarily focused on regulating privacy in specific sectors, such as healthcare, education, and financial institutions. While still important for practitioners to consider, federal privacy regulations have thus far remained largely unchanged by the recent wave of privacy and data regulation activity—although there are pending rulemaking changes that may lead to some change in these rules in 2024. The three major federal privacy laws that regulate specific types of entities—the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and the Family Educational Rights and Privacy Act (FERPA)—have remained stable since at least the last wave of amendments made between 2013 and 2015. All three of these statutes draw heavily on the Fair Information Practice Principles, a set of widely accepted guidelines surrounding the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of personal data. They include, in part:

- Transparency and choice (notice and consent)
- Consumer rights to access and amend their personal information
- Limitations on data collection and use, such as non-disclosure requirements and collection limitation –and–
- Information security safeguards or other breach mitigation procedures

These are not the only statutes that impose requirements on the processing of health, financial, and education data. Many statutes have privacy implications despite not explicitly imposing privacy obligations, such as confidentiality-based requirements. For example, depending on their business, companies should also be aware of the confidentiality requirements in Title I of the Americans with Disabilities Act, the FDA's confidentiality rules during clinical trials, and the Individuals with Disabilities Education Act's medical information confidentiality requirements (in addition to a wide range of state laws that impact the privacy and confidentiality of health data). While practitioners should remain vigilant for developments to the privacy implications of sector-specific statutes that do not directly regulate privacy, the below sections highlight the key considerations in the three most prominent sector-specific privacy laws.

Further, it is important to consider that although federal level legislation has primarily remained unchanged, federal regulators, specifically the Federal Trade Commission (FTC), have responded to evolving privacy and cybersecurity concerns. As such, the below includes a section on the FTC's role in enforcing privacy and cybersecurity violations through its authority to bring actions for unfair or deceptive acts or practices under Section 5 of the FTC Act, 15 U.S.C. § 45.

Health Insurance Portability and Accountability Act

The HIPAA statute itself says little about privacy and security directly but instead creates privacy standards for "covered entities" through the rules developed by the Department of Health and Human Services (HHS). HIPAA establishes a framework of rules governing how specific "covered entities" secure, transmit, and protect "individually identifiable health information." HIPAA requires that covered entities, originally healthcare providers, health insurance plans, and healthcare clearinghouses, comply with a series of rules and standards.

As a result of the HIPAA statute, there are three rules promulgated under HIPAA that practitioners should consider when advising on health information practices:

- The Privacy Rule (45 C.F.R. §§ 160, 164.500–164.534)
- The Security Rule (45 C.F.R. §§ 160, 164.302–164.318)
- The Breach Notification Rule (45 C.F.R. §§ 160, 164.400–164.414)

Under the Privacy Rule, protected health information (PHI) cannot be used or disclosed unless permitted by the rules or specifically authorized by the individual. Entities must respect patients' right to access, amend, and restrict their data, and develop specific procedures to support compliance. There are also specific rules related to the sale of PHI or the use of PHI for marketing. The Privacy Rule is the most expansive in coverage, containing a "mini-security" rule, requiring contracts with business associates which govern their use of PHI, and setting out principles for de-identification of PHI.

The Security Rule builds upon the mini-security provisions in the Privacy Rule and sets forth detailed requirements for the protection of electronic PHI. Covered entities must implement reasonable administrative, physical, and technical safeguards to protect the PHI they process.

Lastly, under the Breach Notification Rule, covered entities must disclose data breaches to both HHS and individuals whose PHI has been compromised. The rule creates the opportunity for affected entities to conduct a risk assessment to determine whether there is a low probability of compromise of the impacted information to avoid these notification obligations.

Notably, the 2009 HITECH Act extended certain elements of the HIPAA rules to reach covered entities' service providers and contractors (called "Business Associates" under the HIPAA rules). Under the HITECH Act, business associates can be directly liable under HIPAA for certain violations, including failing to comply with the Security Rule and failing to provide breach notification to a covered entity or another business associate.

HIPAA serves as a baseline for health information compliance, and explicitly does not preempt more protective state laws. Importantly, HIPAA does *not* cover many entities and types of data involved in the healthcare system, including health apps, fitness trackers, university student health clinics, or most pharmaceutical companies. States have increasingly looked to fill this gap in coverage under HIPAA by passing privacy laws that specifically regulate these categories of health information (as we further detail below).

HIPAA is enforced by HHS, with additional authority in some situations for state attorneys general. For more information on HIPAA enforcement and other general information, see HIPAA Enforcement and Penalties and HIPAA Privacy, Security, Breach Notification, and Other Administrative Simplification Rules.

Family Educational Rights and Privacy Act

The Family Educational Rights and Privacy Act (FERPA) protects the privacy of education records at all schools which receive applicable federal education funds. FERPA gives privacy rights related to education records to the parents of minors and then transfers these rights to the students once they turn 18. Schools must guarantee parents or students access to and the ability to correct errors within the student's educational record and must obtain their consent to release information from that record, although "directory" information such as names or addresses may be disclosed without consent after notifying the student or parent. As under HIPAA, schools are required to include certain limiting contractual provisions in agreements with their service providers. That said, many nonschool entities, such as emerging education technologies (EdTech), receive school data under the "school official exception," which allows a platform to receive personally identifiable information from education records without parental consent if certain criteria are met.

FERPA similarly serves as a baseline, preempting state laws which would allow for disclosure of records not otherwise permissible under FERPA, such as state Freedom of Information laws. Further, states have passed a wide range of student privacy laws, most of which prescribe all or some of the following four requirements: notice and consent, use or collection limitation (particularly in the context of third-party applications or targeted advertising), data breach notification, and deletion. Many states also require that schools extend their privacy obligations via contract to third parties which process or handle student data on behalf of covered entities.

For more general information regarding FERPA, see Family Educational Rights and Privacy Act (FERPA) and Family Educational Rights and Privacy Act (FERPA) Video.

Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA) governs financial institutions and other organizations that offer financial services and products such as financial advising, insurance, or investment. The relevant provisions concerning personal data are generally split into the GLBA Privacy Rule and the GLBA Safeguards Rule. The Privacy Rule requires regulated organizations to both provide detailed notice and

explanation of their information sharing practices and to limit disclosure of nonpublic personal information (NPI). NPI includes information derived from financial transactions, as well as information provided in order to receive financial products or services.

The Privacy Rule requires that financial institutions provide a written privacy notice at the start of their relationship with a customer and annually thereafter. These privacy notices must include, among other requirements:

- An explanation of what information is collected
- Where and with whom the information is shared
- How such information is used
- How the information is protected
- Whether the organization is sharing information with third parties –and–
- Notice of the customer's right to opt out of such sharing with nonaffiliated third parties, subject to certain exceptions

The Safeguards Rule, on the other hand, requires companies to develop, maintain, and implement a comprehensive information security program to keep personal information secure. These provisions require that the written information security program contain administrative, technical, and physical safeguards to protect customer information. For example, under the FTC's Safeguards Rule, an entity must undertake comprehensive risk assessments, appoint a qualified individual to be responsible for the institution's information security program, conduct annual penetration testing of information systems, protect consumer information through encryption, multifactor authentication, and proper storage, and much more.

The FTC recently approved significant modifications to its version of the Safeguards Rule. Among other changes, the new rule will require nonbanking financial institutions regulated by the FTC, including financial technology companies, mortgage brokers, credit counselors, financial planners, and tax preparers, and others, to report certain data breaches and other security events directly to the FTC. This is a meaningful new obligation for GLBA-covered entities regulated by the FTC, and it is possible that other regulators will follow the FTC's lead in this regard.

The GLBA is enforced by various financial regulators that have jurisdiction as the "primary" regulator over the types of financial institutions they regulate. This can range from the Consumer Financial Protection Bureau (CFPB) to the Securities and Exchange Commission (SEC) to state insurance commissioners. These various regulators have released guidance and enforce sector-specific GLBA regulations for the industries they oversee. All other entities that otherwise meet the definition of a "financial institution" as defined under the GLBA but do not fall under the purview of a primary financial regulator fall under the regulatory umbrella of the FTC for GLBA purposes.

For more information regarding the Privacy Rule and Safeguards Rule, see Gramm-Leach-Bliley Act (GLBA) Privacy Requirements and Gramm-Leach-Bliley Act (GLBA) Video.

Federal Trade Commission and General Section 5 Authority

The FTC has jurisdiction over most for-profit organizations and individuals doing business in the United States, other than those in the telecommunications, financial, and transportation industries, which are primarily regulated by other federal agencies. (Note that nonprofits are generally excluded from the FTC's jurisdiction.) 15 U.S.C. § 45(a). The FTC Act was established to regulate questionable business practices and protect consumers. Specifically, Section 5 of the FTC Act prohibits unfair or deceptive acts and practices in commerce, which can include consumer privacy violations and engaging in improper data collection, use, and disclosure practices. 15 U.S.C. § 45. Section 5 is also routinely applied to penalize organizations that do not have reasonable data security practices. As such, the FTC can bring enforcement actions for Section 5 violations. Notably, practices inconsistent with FTC guidance have the potential to result in corrective action by the Commission under Section 5 if the Commission finds those practices to be unfair or deceptive after an investigation.

Individuals or companies responsible for the collection, storage, use, disclosure, or other processing of personal information should ensure that those activities do not violate Section 5's prohibition on unfair or deceptive acts or practices.

The FTC uses a three-part test to determine whether an act or practice is deceptive:

- The representation, omission, or practice must mislead or be likely to mislead the consumer.
- The consumer's interpretation of the representation, omission, or practice must be reasonable under the circumstances.
- The misleading representation, omission, or practice must be material.

See FTC Policy Statement on Deception.

To avoid liability under a deception theory, companies should ensure that statements, including those regarding their practices, do not mislead a consumer in any material

way. Further, companies should remain consistent with the promises made to consumers about the collection, use, storage, or dissemination of personal information. The FTC has consistently enforced the "deceptive" prong of Section 5 for privacy violations, including in 2023 with enforcement actions against companies such as GoodRx, BetterHelp, and Vitagene. See Federal Trade Commission (FTC) Consumer Privacy Enforcement Tracker. All of these enforcement actions alleged that these companies failed to uphold the promises they made to consumers regarding how their data was being used or disclosed (in addition to other violations).

In determining whether an act or practice is unfair, the FTC requires that the act or practice "cause{} or {be} likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). In determining whether an act or practice is unfair, the FTC "may consider established public policies," but "[s]uch public policy considerations may not serve as a primary basis for [a determination of unfairness]." 15 U.S.C. § 45(n). The FTC has historically relied on the unfairness test in the context of enforcement actions involving companies' misuse of consumer data and, in recent years, has adopted an increasingly broad view of what constitutes unfairness in this sphere, sweeping in such practices as inadequate cybersecurity controls and unnecessary retention of customer data, among others.

The FTC was particularly active in 2023 in using the "unfairness" prong of Section 5 to bring enforcement actions against companies for alleged privacy violations. For example, in the GoodRx and BetterHelp cases (referenced above), the FTC alleged that, not only was the sharing of sensitive consumer health information for targeted advertising purposes in violation of the promises made by these companies, it was also an "unfair" practice because these companies did not obtain consumers' affirmative consent prior to disclosing their health information for this purpose. The implication of the FTC using the "unfairness" prong instead of the "deceptive" prong of Section 5 for privacy enforcement actions is that the FTC is essentially creating new substantive privacy compliance requirements for all companies, regardless of the disclosures they make in their privacy policies or other publicly available documents. The FTC has historically taken this approach with its data security enforcement cases (and continues to do so) but has now expanded this framework to its privacy cases.

The FTC also regularly issues guidance that can provide practitioners insight on how the FTC views certain issues. For example, in 2023, the FTC issued guidance on how companies can better protect health information, as well as how companies can avoid misusing biometric data. These guidance documents, inspired by recent FTC enforcement actions, indicate where the agency is likely to focus its attention in the future.

Use Case-Specific Privacy Laws

In addition to these sector-specific privacy laws, the U.S. has also historically regulated privacy by focusing on specific use cases of personal information. These include the use of personal information for telemarketing, targeted advertising, consumer reports, clinical trials, breach notification, and in certain cases for selling personal information (as a data broker).

Telemarketing

Statutes governing automated marketing messages have existed for at least two decades. Under the Telephone Consumer Protection Act (TCPA) of 1991, 47 U.S.C. § 227, the Federal Communications Commission (FCC) regulates the use of automated calling, text messages, and other telephone solicitations. Importantly, though the FCC is the main regulatory body responsible for enforcement under the TCPA, practitioners should note that this statute also has a private right of action and uncapped statutory damages of $500 per call made in violation of the statute. This creates the potential for substantial class action liability. Further, the 2019 Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED) strengthened FCC enforcement obligations and heightened the intentional violation penalty to $10,000 per call.

The TCPA requires businesses which use either equipment that has the capacity to store or produce telephone numbers using a number generator (autodialer) or which use prerecorded calls to obtain express written consent before calling an individual at a wireless number. The TCPA specifically bars autodialers from engaging multiple lines of a business with multiple phonelines or using autodialers to determine if a line was a telephone or voice line. The TCPA provides exemptions for messages related to specific subjects, such as calls and texts from wireless carriers to customers, time-sensitive messages subject to HIPAA or relating to data breaches, and package delivery alerts. Prerecorded calls face similar rules, requiring express consent from an individual before calling unless the call is for emergency purposes, made on behalf of a nonprofit entity, or delivers a healthcare message. For more information regarding TCPA compliance, see Telephone Consumer Protection Act (TCPA) Compliance and Telephone Consumer Protection Act (TCPA) Overview Video.

Companies should be aware that express consent has been a subject of several clarifications by the FCC. The

FCC initially held that providing a phone number, without instructions to the contrary, was sufficient to provide express consent for calls regarding that transaction, even from third parties. Further guidance held that where individuals provide a telephone number to a HIPAA-covered provider, they have also consented to messages from or on behalf of that covered entity and its business associates. Individuals may also revoke consent through reasonable means. For more information, see TCPA Reference Guide (Autodialed or Prerecorded Voice Calls and Text Messages), Prior Express Written Consent under TCPA Rules Checklist, and Telephone Consumer Protection Act: Prior Express Written Consent Rules Video.

States additionally have their own statutory requirements for telemarketing, including stricter definitions of abusive practices, requirements for permission to continue the call, or state do-not-call registries with harsher penalties than the federal registry. For more detailed information, see Telemarketing Privacy State Law Survey.

The 2003 Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM), 15 U.S.C. §§ 7701–7713, regulates emails. CAN-SPAM requires businesses which send or pay for the sending of "commercial" emails (initiators) to ensure that emails, among other requirements:

- Contain no false or misleading header information (e.g., the sender's email and subject information)
- Clearly and accurately identify the initiator
- Include an opt-out mechanism (initiators who are advertising their own services (senders) are further required to process and honor opt-out requests)
- Include the sender's valid physical postal address –and–
- Identify the message as an advertisement or solicitation

CAN-SPAM is mainly enforced by the FTC, but state attorneys general and other state agencies may also bring claims seeking injunctive relief, statutory damages, or fees. For more information regarding CAN-SPAM, see CAN-SPAM Act Compliance and Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM) Video.

Targeted Advertising

Targeted advertising—advertisements tailored for a specific audience based on the particular audience's traits, such as demographics, lifestyle, or interests—represents an important evolution in digital marketing. Companies that engage in targeted marketing are able to leverage the data that they collect from their consumers, as well as through data brokers, to gain insights into the consumers' interests and personalize consumers' advertising experience.

The federal legislature has not regulated in the targeted advertising space. However, companies and practitioners which are interested in proactive compliance in this space can look to industry standard guiding principles provided by the Digital Advertising Alliance (DAA) and Network Advertising Initiative (NAI).

The NAI, which has received support from the FTC, provides self-regulatory codes that establish data management practices with respect to the collection of tailored advertising. Specifically, the codes outline notice, choice, accountability, data security, and use limitation requirements for NAI member companies. Further, the DAA, an independent not-for-profit organization which establishes and enforces responsible privacy practices for relevant digital advertising, has established guiding principles which promote transparency and control for users across devices, as well as principles that focus on online behavioral advertising, multi-site data, and mobile environments. Although these principles are nonbinding, the DAA and NAI enforce compliance with the described principles for members and serve as a guide for self-regulation when engaging in targeted advertising.

Further, legislation in the targeted advertising space continues to evolve. States such as California and Virginia have passed comprehensive privacy laws that outline specific requirements for entities which engage in targeted advertising. For example, the California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100 et seq., as well as other state privacy laws, requires that covered entities provide consumers the opportunity to opt out of the sharing or sale of their personal information for the purpose of targeted advertising.

Clinical Trials

Clinical trials consist of a research study in which human subjects are prospectively assigned to one or more interventions (which may include placebos or other controls) to evaluate the effects of those interventions on health-related biomedical or behavioral outcomes. Clinical trials, and any other federal research involving human subjects, have been governed by a multiagency "common rule" since 1991. That rule was substantially revised in 2018. The rule establishes the core procedures for human research subject protections, which include obtaining informed consent and review by an Institutional Review Board (IRB), as well as particular protections for vulnerable groups like children and pregnant women. 28 C.F.R. §§ 46.101 –46.124. The amendments added disclosure and explanation requirements to the informed consent process, allowed researchers to seek broad consent for both current research and future research using the same data or biospecimens provided they disclose certain facts, clarified the scope of research

exempt from the common rule, streamlined the IRB process for cooperative research, and clarified the IRB's authority to monitor ongoing review of research.

The nature of clinical trials gives rise to important privacy considerations. As such, organizations which conduct clinical trials should pay close attention to their information-related practices.

Consumer Reports

The Fair Credit Reporting Act of 1973 (FCRA), 15 U.S.C. § 1681 et seq., regulates the collection, transmission, and use of private consumer data (including credit information) and serves to protect consumers from the negligent or willful inclusion of inaccurate information in consumer reports. It primarily imposes obligations on consumer reporting agencies (CRAs) that compile private information into consumer reports used to make eligibility decisions for credit, employment, insurance, housing, and similar decisions. CRAs generally include credit bureaus and employment or tenant background screening organizations, among others. CRAs must make required disclosures to consumers upon request, implement reasonable procedures to ensure proper identification, properly maintain consumer files, resolve accuracy disputes with consumers, provide reports only for legitimate purposes, and train personnel to explain information furnished to consumers. Furnishers, or entities which provide consumer information to CRAs, have an obligation to provide CRAs with accurate information, notify consumers if they have furnished negative information, and to investigate disputes directly filed with them. Users are typically required to provide notice to and obtain consent from the subjects of such reports. Further, debt collectors are bound by specific rules and must respect consumer privacy rights enumerated by the Fair Debt Collection Practices Act (FDCPA). The FCRA is enforced by the FTC and CFPB, as well as other financial regulatory institutions.

Like the other federal statutes, the FCRA does not preempt stricter state laws. As such, a few states have their own "mini-FCRA" laws, while others have implemented specific requirements for particular consumer reporting inquiries. For more information on state-level statutes, see Fair Credit Reporting Act (FCRA) and State Mini-FCRAs: Step-by-Step Guidance for Compliance and Screening and Hiring State Practice Notes Chart.

For more information regarding FCRA, see Fair Credit Reporting Act, Consumer Reports and Credit History Checks under the Fair Credit Reporting Act (FCRA), and Fair Credit Reporting Act (FCRA) Video.

Data Brokers

Data brokers are businesses that collect consumers' personal information and resell it to third parties. Practitioners should be aware of how data brokers operate as well as the relevant laws and guidelines that apply to data brokers. Since the FTC's seminal report on data brokers in 2014, an increasing number of states have passed laws specifically regulating the practices of companies which collect personal information and resell it to third parties. The report provides a set of best practices for brokers, including taking privacy into account during the entire product design process (privacy-by-design), limiting collection of children's data, and ensuring downstream data is not used for discriminatory or fraudulent purposes. Companies should note that the FTC guidance emphasizes transparency and disclosure. Similarly, at the state level, statutes have focused on regulating data brokers' disclosures regarding their information practices. Thus far, no statute has provided a private right of action, leaving enforcement up to the attorney general's office (although California has recently provided for enforcement by its privacy regulator—the California Privacy Protection Agency. Cal. Civ. Code § 1798.99.82(c)).

Currently, only California, Vermont, Oregon, and Texas have passed laws specifically regulating data brokers, while Nevada has expanded its general online data privacy law to cover data brokers. The laws differ somewhat in their scope and applicability. California and Vermont similarly define data brokers as businesses which collect and sell information on individuals with whom they do not have a direct business relationship, but Vermont's definition also includes licensing data. See Cal. Civ. Code § 1798.99.80(c) and Vt. Stat. Ann. Tit. 9, § 2430(4)(A). Under Oregon's law, effective Jan. 1, 2024, the definition of data broker does not specify a "direct business relationship," instead applying to anyone who sells information to another person. ORS § ___.___ [Added by 2023 c. 395 § 1(1)(c)(A)]. The Nevada law has a similar definition but adds the requirement that data brokerage must be the *primary* business of that entity. Nev. Rev. Stat. Ann. § 603A.323. The Texas law, meanwhile, adopts a distinct approach, defining "data broker" as "a business entity whose principal source of revenue is derived from the collecting, processing, or transferring of personal data that the entity did not collect directly from the individual linked or linkable to the data," then defining revenue and personal data processing thresholds that govern whether an entity is subject to the law. 2023 Tex. SB 2105, 2023 Tex. Gen. Laws 963.

The state data broker laws (and Nevada's general online data privacy law) differ in several other notable

respects. The California, Vermont, Oregon, and Texas laws require data brokers to register with the state and make information associated with their registration, such as their address and other business information, publicly available, while Nevada only requires that data brokers maintain an address to receive opt-out requests. Further, in California, Vermont, and Texas, data brokers must also implement an information security program that protects personally identifiable information through administrative, technical, and physical safeguards. Lastly, Vermont's data broker law also requires that organizations publish a statement specifying details like the types of data collection and activities that a user may not opt out from, and a statement about whether the data broker uses a purchaser credentialing process. Relatedly, Oregon requires that data brokers submit a declaration which provides consumers with any relevant opt-out information, while California's law allows for optional submission of additional information.

Looking ahead, practitioners should be aware that the California "Delete Act," 2023 CA S.B. 362, amending the California data broker law, took partial effect on Jan. 1, 2024. The Delete Act heightened data brokers' reporting requirements and penalties for violations, as well as empowered the California Privacy Protection Agency to create a system to allow consumers to make a single data deletion request that is binding on all data brokers registered in California. For more information on California requirements and the Delete Act, see Data Broker Compliance and Enforcement Checklist (CA).

Data brokers and their advisors should also consider the increasing likelihood of enforcement action at the state level under state Unfair and Deceptive Acts and Practices (UDAP) statutes, which can result in significant fines. For example, nearly every state attorney general participated in a settlement with Equifax over its 2017 data breach. As a result, Equifax agreed to pay $600 million to settle allegations that it failed to safeguard the sensitive personal information of almost 150 million people.

Finally, data brokers should be cognizant of potential future regulation at the federal level by the CFPB. In March 2023, the CFPB issued a Request for Information regarding data broker practices, which it stated would be used to inform future rulemaking under the FCRA.

Data Breach Laws

All 50 states and the U.S. territories have laws that require private or government organizations to notify individuals and (frequently) state attorneys general of data security breaches that impact their personal information. Security breach statutes all require notification to affected residents without unreasonable delay and specify who must comply with the law, the scope of personal information covered under the law, what qualifies as a data breach, notice requirements, and exceptions to the law. However, the requirements of each particular state law vary substantially, with some states not requiring notice to governmental bodies, others not requiring notification of credit reporting agencies, and varying sets of obligations with regards to the contents of the notification and the time frame within which notice must be delivered. As such, compliance with state privacy laws will require discerning state-level requirements in preparation of a data breach, and practice will heavily depend on the state.

For more information on data breach notification requirements, see Data Breach Notification Resource Kit, Data Breach Notification State Law Survey, and Data Breach Planning and Management.

FTC Guidance on Data Breaches Which Implicate Health Information

The Federal Trade Commission (FTC) enforces the Health Breach Notification Rule (HBNR) for vendors of personal health records and their service providers. Vendors of personal health information include companies that offer or maintain personal health records. For example, covered entities could include a fitness tracker app, or health app that collects information from consumers and can sync with a consumer's fitness tracker. Additionally, service providers of a covered entity, such as a data storage provider or billing company, are also subject to the HBNR.

Practitioners should pay close attention to their disclosure practices around sensitive information and ensure compliance under this rule, as the FTC remains focused on enforcement in this area. For example, the FTC recently obtained a settlement from GoodRx, a prescription drug discount and telehealth platform, for allegedly sharing users' personal health information with third parties without properly disclosing their data practices or obtaining users' affirmative consent, as well as for failing to maintain adequate policies or procedures to protect users' personal health information. This rule applies to breaches of *identifiable* health information that is unencrypted or intact. Companies such as period tracking apps, fitness trackers, or diet apps, may find themselves subject to both state data breach laws and FTC regulation, depending on the type of data they collect.

Data-Specific Privacy Laws

Most recent developments in data-specific privacy laws have arisen at the state level. Laws that regulate health information and health-adjacent types of data have dominated recently established regulations at the state level. Other states have begun adopting biometric privacy

protection laws, first pioneered by Illinois, albeit frequently without the Illinois law's private right of action. Further, state laws imposing heightened HIPAA non-disclosure obligations have been further augmented by statutes creating particular privacy requirements for genetic information and medical information.

At the federal level, the privacy legal framework is structured around a series of long-standing data-specific privacy laws. These laws govern the disclosure of specific types of personal information ranging from video rental history to the information collected from specific individuals, such as children. Finally, there are also self-regulatory standards that companies should be aware of, especially if they process payment card data in the ordinary course of business.

Biometrics

Three states—Illinois, Texas, and Washington—have passed laws specifically regulating biometric information. The definitions of biometric identifiers in these laws vary but generally include data elements such as retina scans, iris scans, fingerprints, voiceprints, and facial geometry. These laws require businesses to provide notice and obtain consent prior to collecting and sharing biometric information and also require businesses to implement data retention policies in relation to biometric identifiers. Of the three states with biometric laws, Illinois's Biometric Information Privacy Act (BIPA) has the most requirements. BIPA is also heavily litigated because it has a private right of action, along with statutory damages and allowance for attorney's fees. In 2023, many state legislatures considered biometric privacy bills, each proposal with varying levels of requirements and enforcement, but none ultimately passed and become law. For more information, see Biometric Privacy State Law Survey, Biometric Privacy State Legislation Tracker (2023-2024), Biometric Privacy: Overview Video, and Biometric Privacy and Artificial Intelligence Legal Developments.

In addition to these specific biometric information laws, state legislatures are increasingly choosing to regulate biometric information through mechanisms beyond data-specific laws. The comprehensive privacy laws referenced below (such as the CCPA and the Colorado Privacy Act (CPA)) all regulate biometric information in some form. State data breach notice laws are also expanding to include biometric information in their definition of personal information.

Additionally, in 2022, a variety of state and local governments considered and adopted laws restricting the use of specific technologies that facilitate the collection of biometric information, such as facial recognition technologies. While the momentum across the U.S. has since slowed, states are likely to follow the trend set by the European Parliament's recent adoption of the Artificial Intelligence Act (AI Act) governing the use of artificial intelligence systems such as many facial recognition technologies.

Genetic Information

The majority of state legislatures follow a policy of genetic exceptionalism, which applies special protections to genetic information. Similar to HIPAA's approach to regulating health information, early genetic privacy laws approached the regulation of genetic information through imposing disclosure limitations or the extension of property rights to genetic samples. However, in response to the increasing popularity of direct-to-consumer (DTC) genetic testing, newer bills specifically dealing with the protection of genetic information have surged through state legislatures. See State Lawmakers Find Success with Genetic Privacy. These new laws focus on creating a framework for regulating genetic information which is more in line with HIPAA norms. The laws include various privacy-based obligations, such as requiring notification of privacy policies, consent for data use, and consumer rights of access and deletion, as well as stiffening penalties for unauthorized use, transfer, or analysis of genetic information. The state laws also provide some degree of exemptions for clinical research, for de-identified data, and for PHI already covered by HIPAA.

It is important to note that state laws share many similarities but have substantial variation in the scope of their coverage and the breadth of their research exemptions. For example, California and Utah's Genetic Information Privacy Acts further introduce an obligation to de-identify collected data. See Cal. Civ. Code § 56.18 et seq., and Utah Code Ann. § 13-60-101 et seq. Florida and Alaska's genetic information laws are unusual, as they impose criminal, rather than civil penalties for violations. See Fla. Stat. § 760.40 et seq., and Alaska Stat. § 18.13.010 et seq. Further, some state-level regulations also extend beyond DTC genetic testing companies to cover all individuals, including healthcare providers who do not qualify for the law's research exceptions.

Genetic information is also regulated at the federal level by the Genetic Information Nondiscrimination Act of 2008 (GINA), See 110 Pub. L. No. 233, 122 Stat. 881. Broadly speaking, GINA protects individuals from discrimination on the basis of genetic information in the areas of health insurance coverage and employment. Title I of GINA prohibits genetic discrimination in health insurance coverage, including adjusting premiums on the basis of genetic information and collecting genetic information for underwriting purposes or prior to an individual's enrollment

in a health insurance plan. Title II, meanwhile, prohibits genetic discrimination in the employment context, including in hiring, compensation, and terms, conditions, and privileges of employment. Title II also prohibits employers from acquiring employee genetic information (as well as genetic information of family members), subject to specified exceptions, and places confidentiality restrictions on genetic information that employers *can* permissibly collect.

Consumer Health Data

In 2023, Washington, Connecticut, and Nevada each passed laws imposing new requirements for the collection, use, and sale of consumer health data. The enactment of these laws focused on regulating health information at the state level constitutes a major development in the U.S. state privacy law landscape.

Broadly, these new laws cover "consumer health data," a broad term which includes biometric data, measurements of bodily functions or vital signs, or any other health status identifying data. Washington's law provides the broadest definition of the term, extending to *any* personal information which identifies health status, while the Nevada and Connecticut statutes only cover data *used by* an entity to identify health status. 2023 Wa. HB 1155; 2023 Nev. SB 370; 2023 Ct. SB 3. These laws, much like obligations created under HIPAA, create a list of new requirements for companies that process consumer health data such as provision of privacy policies, limitations on when data can be processed, rights to access relevant data, and prohibitions on sharing without explicit written consent. Note, however, that these laws are also exclusive from HIPAA because they all include exemptions for PHI that is processed pursuant to HIPAA (they are specifically intended to apply to non-HIPAA health data).

Notably, the Washington and Nevada laws break from the HIPAA framework in that they require *separate and distinct* consents for collection and sharing of health data, rather than the unified consent previously permitted. Further, all three bills prescribe limitations on specific types of data that could be used to infer health data. For example, these laws all limit the use of geofence tracking or precise geolocation data near healthcare-related facilities. Companies that handle consumer health data and counsel should be aware of these requirements. Violations could give rise to action by state attorneys general. Further, the Washington law contains a private right of action for violations, which could lead to substantial legal exposure.

The Video Privacy Protection Act and the Drivers Privacy Protection Act

At the federal level, the Video Privacy Protection Act (VPPA), 18 U.S.C. § 2710, and the Drivers Privacy Protection Act (DPPA), 18 U.S.C. §§ 2721–2725, were passed in response to public outcry over access to specific data. The VPPA prohibits those involved in the sale, rental, or delivery of video or audio cassettes from disclosing the personally identifiable information of their customers. Since its implementation, the language of the VPPA has served as a springboard for a variety of cases against streaming services. Recently, this statute has provided a legal avenue for complaints against websites which provide video and collect advertising data using site activity tracking tools, demonstrating a reemergence of the VPPA's relevance in privacy class action litigation. The DPPA, as the name suggests, requires state departments of motor vehicles (DMVs) to safeguard personally identifiable information of drivers and prohibits disclosures of such information outside of a specifically defined range of acceptable uses. Unlike the VPPA, the DPPA explicitly limits applications of its requirements to the information collected by DMVs. As such, it has not had as great an impact on the privacy landscape as other legislation.

Children's Data

The Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501–6506, imposes rules and restrictions on operators of websites or mobile applications that collect personal information online from children under the age of 13. To comply with COPPA, entities that collect personal information from children must (among other things) (1) provide consumers with a clear and prominent link to the company's applicable privacy policy, and (2) provide direct notice to and obtain (with limited exceptions) prior consent from parents for any such collection. This consent cannot be obtained through text, parental controls permissions, or electronic signatures, but rather must meet standards for verifiability set by the FTC. Once the information is collected, the entity is obligated to secure that information, carefully vet the service providers it allows to access the data, and give parents control over ongoing collection, retention, and use of that information. COPPA covers any provider of online services directed at children which collects personal information from children, as well as operators of general services who know they collect, use, or disclose personal information from children under 13. As such, regulated entities can range from a website to a video game console.

Companies should pay close attention and continuously evaluate whether they are subject to COPPA obligations, as violations can give rise to FTC enforcement actions and significant civil penalties. In 2023, the FTC announced a $20 million settlement against Microsoft over allegations that Microsoft's data privacy practices, in connection with its Xbox Live offering, knowingly violated COPPA by failing

to provide complete and direct notice—both prior to and after it collected, used, and disclosed children's information. Practitioners should note that the FTC's commentary on the resulting requirements imposed on Microsoft indicates that the FTC remains focused on all types of covered entities, including third parties "with actual knowledge" of collected children's information, not just those who direct their services towards children.

Notably, COPPA includes a safe harbor provision, allowing entities to follow commission-approved third-party regulatory frameworks rather than the FTC's enforced regulations. For more information regarding COPPA, see Children's Online Privacy Protection Act (COPPA) Compliance.

Following the state-led trend of privacy law's recent evolution, California has also passed laws protecting children's information. The California Age-Appropriate Design Code Act, 2022 Cal AB 2273, imposes a number of affirmative requirements on businesses in addition to prohibiting certain data practices regarding children's information. Covered entities include businesses that provide online services, products, or features likely to be accessed by children under 18. Covered entities must implement:

- Age assurance systems appropriate to the level of risk
- Data protection impact assessments
- Default settings that offer a high level of privacy –and–
- Age-tailored transparency requirements

Further, many state comprehensive privacy laws regulate children's information as sensitive information. As such, companies that process children's information should remain attentive of evolving regulations at the state level.

Payment Card Data

Every day, individuals across the globe share payment card information, including their name, card number, expiration date, and security code. Naturally, the practices around payment card information have raised privacy and security concerns. As such, four major credit card companies have created a global independent body known as the PCI Security Standards Council (the Council). The Council has promulgated the Payment Card Industry Data Security Standards (PCI-DSS rules), which establish data security standards for all businesses, regardless of size, that process credit card information. In response to the rise of credit card use and fraud, the rules aim to reduce the instances of fraud and related privacy concerns by providing a baseline for security standards for related processing, collection, and storage. The standards include, among others, requirements around installing firewalls, password strength, encryption of transmission, and tracking and monitoring access to payment networks. As such, businesses that process credit card information should be aware of these data-specific rules.

State Comprehensive Privacy Laws

In recent years, some states have attempted to fill the gap left by a lack of a federal data privacy law by passing their own versions of comprehensive privacy laws. In the absence of a comprehensive federal privacy law, California—the first state to pass comprehensive privacy legislation—drew inspiration from international privacy frameworks such as the General Data Protection Regulation (GDPR). Since then, California has been joined by Virginia, Colorado, Utah, Connecticut, Iowa, Tennessee, Indiana, Texas, Oregon, Delaware, and Montana.

California (CCPA/CPRA)

Similar to other states' laws, the California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code § 1798.100 et seq., as amended by the California Privacy Rights Act of 2020 (CPRA) (collectively, the CCPA), requires that businesses which process personal information and meet certain revenue and information-processing thresholds disclose their data privacy practices through consumer-facing privacy policies. The CCPA also requires covered entities to meet consumer data requests, such as requests by consumers to know what personal information a business collects about them, to delete and correct that information, and to opt-out of certain types of data processing.

Despite the privacy laws that followed, the CCPA remains one of the most prescriptive as it provides companies with specific compliance metrics and requirements. Many states require covered entities to provide an opt-out right to consumers for specific information practices and uses. However, the CCPA requires that companies establish certain mechanisms to comply under the law. For example, under the CCPA, businesses that engage in the sale or sharing of personal information must provide notice to consumers of these information practices, like under other state laws. However, CCPA-covered businesses must also provide a "Do Not Sell or Share My Personal Information" link on their website to ensure that users have a clear manner to exercise their right to opt out of the sale or sharing of their personal information. As such, companies and practitioners examining state privacy law compliance may choose to begin with assessing CCPA compliance, as it remains a detailed compliance regime. For more information on the CCPA, see California Consumer Privacy Resource Kit (CCPA and CPRA) and California Consumer Privacy Compliance (CCPA and CPRA).

Colorado Privacy Act

In June 2021, Colorado became the third state to join the patchwork of laws in the United States when its legislature passed the Colorado Privacy Act (CPA). Colo. Rev. Stat. § 6-1-1301 through 6-1-1313. Similar to the amendments to the CCPA made by the CPRA and accompanying regulations, the Colorado Attorney General has promulgated the Colorado Privacy Act Rules (CPA Rules) that clarify and expand upon the requirements articulated in the CPA. Notably, the CPA Rules go beyond the CCPA by addressing profiling and data protection assessments—topics that California regulators are only beginning to consider. Further, the CPA Rules provide detailed guidelines for companies as they evaluate consent. See 4 Colo. Code Regs. § 904-3, Rules 7.01 through 7.09. The CPA regulates profiling, which means any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements. Colo. Rev. Stat. § 6-1-1303(20); 4 Colo. Code Regs. § 904-3, Rule 2.02. Under the CPA Rules, controllers that engage in the processing of personal data for the purpose of profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer, must provide specific profiling-related disclosures in their privacy notices regarding certain automated decisions, specifically:

- What decisions are subject to profiling
- The categories of personal data that were or will be processed as part of the profiling
- A non-technical, plain language explanation of the logic used in the profiling process
- A non-technical, plain language explanation of how profiling is used in the decision-making process, including the role of human involvement, if any
- If the system has been evaluated for accuracy, fairness, or bias, including the impact of the use of sensitive data, and the outcome of any such evaluation
- The benefits and potential consequences of the decision based on the profiling –and–
- Information about how a consumer may exercise the right to opt out of the processing of personal data concerning the consumer for profiling

4 Colo. Code Regs. § 904-3, Rule 9.03.

Further, the CPA also requires that controllers conduct data protection assessments for processing activities that present a "heightened risk of harm" to consumers. Colo. Rev. Stat. § 6-1-1309(2). The CPA Rules expand on the content that these assessments must include and provide details about the timing of these assessments. A controller must review and update the data protection assessment as often as appropriate, considering the type, amount, and sensitivity of personal data processed and level of risk presented by the processing throughout the processing activity's life cycle in order to: 1) monitor for harm caused by the processing and adjust safeguards accordingly, and (2) ensure that data protection and privacy are considered as the controller makes new decisions with respect to the processing. 4 Colo. Code Regs. § 904-3, Rule 8.05(B). The CPA Rules provide further guidelines for controllers regarding the timing of these assessments. For example, companies which engage in the previously described profiling activities must update their data protection assessments at least annually. 4 Colo. Code Regs. § 904-3, Rule 8.05(C).

The CPA Rules also comprehensively address user consent, and in particular devote an entire section to the concept of dark patterns, providing a series of nine principles that controllers should consider when designing a user interface or a choice architecture used to obtain consent. These principles include, in part, the presentation of symmetrical choices, avoidance of emotionally manipulative language or visuals, not using preselected or default options, and considering the unique characteristics of the target audience. 4 Colo. Code Regs. § 904-3, Rule 7.09(A).

While companies can leverage their CCPA-specific compliance programs to align with many of the Colorado requirements, the overlap will not be comprehensive given the CPA Rules' extensive guidelines, specifically in the areas of automated decision-making, impact assessments, and consent. As such, a key step in compliance with developing state privacy laws will require companies to pay close attention to the CPA and its rules.

For more information on the Colorado law, see Consumer Data Privacy (CO) and Colorado Privacy Act (CPA) Compliance.

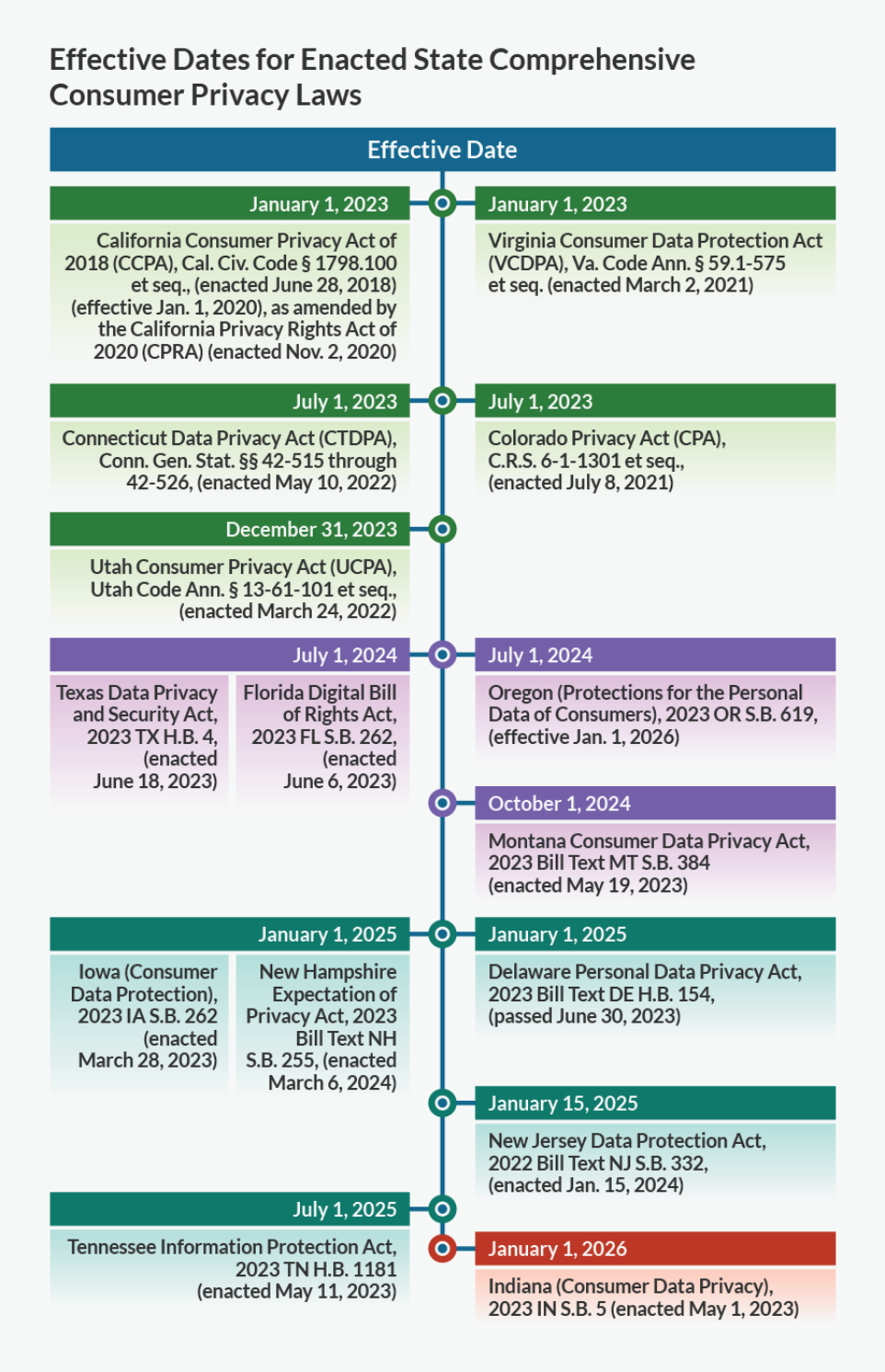
Other States

In addition to California and Colorado, 10 other states have enacted comprehensive privacy laws and one state (Florida) has passed a more limited version of a comprehensive privacy law that only applies to certain large-scale data processors. All of the non-California state comprehensive privacy laws are relatively similar to one another—they all include individual consumer rights, notice and privacy policy requirements for businesses, and special protections for sensitive data. They also apply similar definitions of personal data. However, they also vary in some ways. For example, some state laws have narrower exemptions than others and include more extensive categories of information in terms of what they regulate as "sensitive."

Of the newly passed state laws, Delaware, Connecticut, and Oregon have stronger privacy protections for consumers by

including obligations around certain types of information practices such as dark patterns, sensitive data, recognition of opt-out settings, and providing opt-out requirements for certain processing activities. In comparison, Iowa's law is likely the least restrictive of recent privacy statutes, as it does not provide, for example, the rights to correct or opt out of certain processing (such as profiling).

As privacy law continues to evolve at the state level, practitioners should pay close attention to each state's compliance requirements and their varying effective timelines. In addition to California and Colorado, the Virginia, Utah, and Connecticut laws are in effect. Additionally, state comprehensive privacy laws in Texas, Oregon, and Montana (as well as Florida's more limited law) will take effect in 2024. See the chart below for more effective dates.



For more information on how state comprehensive consumer privacy laws compare, see the Consumer Data Privacy topic in the Data Security & Privacy State Law Comparison Tool. You can also track consumer privacy legislation with the Privacy Legislation Tracker: State Comprehensive Consumer Privacy Bills (2024).

Future of Privacy Law

Privacy professionals should remain aware of new legal developments that might affect their matters. Practitioners need to understand whether and how sector, industry, data-specific, and comprehensive privacy laws apply to a particular matter and how to reconcile different legal requirements. At the state level, privacy professionals should be aware of developments in state data-specific laws, as they represent a novel step in the privacy landscape and bring new compliance requirements. Although the recurring similarities among new comprehensive state privacy laws suggest that a consensus framework is beginning to emerge, practitioners should be aware of state-specific variations in the extent of rights, scope of coverage, and precise procedural requirements, such as in California and Colorado. Finally, practitioners should pay close attention to enforcement actions brought by the FTC and other regulators involving privacy compliance as those will provide insight into how regulators are approaching novel privacy issues.

Kirk Nahra, Partner, WilmerHale

Kirk Nahra has been a leading authority on privacy and cybersecurity matters for more than two decades. He co-chairs the firm's Cybersecurity and Privacy Practice as well as the Artificial Intelligence Practice. In recognition of his professional work in these areas, he was named the winner of the 2021 Vanguard Award from the International Association of Privacy Professionals (IAPP)—one of the most prestigious in the privacy field—which recognizes one IAPP member each year who demonstrates exceptional leadership, knowledge and creativity in privacy and data protection.

Mr. Nahra counsels clients across industries, from Fortune 500 companies to startups, on implementing the requirements of privacy and data security laws across the country and internationally, and he advocates for clients experiencing privacy and security breaches. Mr. Nahra also represents clients in contract and transactional matters, enforcement actions, litigation and investigations related to a wide range of issues before the Federal Trade Commission (FTC), the US Department of Health and Human Services (HHS) Office for Civil Rights, and other state and federal privacy and security regulators. He also represents a wide range of companies across industries on the growing array of complicated legal issues involved in artificial intelligence, including issues involving governance, data rights, data integrity and a wide range of investigation and compliance issues.

Arianna Evers, Special Counsel, WilmerHale

Arianna Evers helps clients navigate privacy, cybersecurity and artificial intelligence (AI)-related challenges in an increasingly complex and fluid legal environment. Ms. Evers represents clients in high-stakes enforcement actions with regulators, including the Federal Trade Commission (FTC), state attorneys general, and the US Department of Health and Human Services Office for Civil Rights (HHS-OCR), as well as in litigation in state and federal courts, concerning alleged privacy and consumer protection violations. She also advises clients on incident preparedness and response, and manages data breach investigations, overseeing privileged forensic work and notice to regulators, affected individuals and contracting parties for clients across a variety of sectors and industries.

A significant portion of Ms. Evers's practice involves advising clients on their development and use of AI and other emerging technologies. Ms. Evers provides clients with a thoughtful but practical approach to managing legal and reputational risks in an area with a tremendous amount of legal uncertainty. She has advised clients building foundation AI models as well as those looking to leverage AI in their products, services, and day-to-day operations on implementation concerns, data privacy risks, cybersecurity, governance and appropriate policies, risk management, fairness, and discrimination.

Ali Jessani, Senior Associate, WilmerHale

Ali A. Jessani counsels clients on privacy, cybersecurity and other regulatory risks related to data protection. He has particular experience advising companies on US state privacy compliance, including the California Privacy Rights Act and other comprehensive state privacy laws, and issues related to health privacy, including the Health Insurance Portability and Accountability Act (HIPAA) and state laws regulating non-HIPAA health data. His other areas of experience include advising clients on compliance with the Federal Trade Commission Act, international privacy obligations (including the General Data Protection Regulation), financial privacy laws and issues related to employee data, targeted advertising and biometrics. Mr. Jessani's clients include healthcare organizations, data analytics providers, advertising agencies, social media platforms, large financial institutions, B2B companies, start-ups experimenting with cutting-edge technology and non-profits.

Mr. Jessani's experience spans drafting policies and contracts, assisting with transactional matters, negotiating with counterparties on data issues, and providing practical, risk-based advice to his clients regarding their compliance obligations. He also guides companies with respect to their legal obligations after security incidents, as well as through state and federal regulatory investigations related to data protection. Mr. Jessani routinely provides counsel to clients on challenges related to emerging technologies, including artificial intelligence (AI) and generative AI specifically, and advises companies on how they can adopt new and proposed uses of consumer information while accounting for issues related to data rights, integrity and governance.

Genesis Ruano, Associate, WilmerHale

Genesis Ruano counsels clients on cybersecurity, privacy, and regulatory risks.

Prior to joining the firm, Ms. Ruano worked as a student attorney and teaching assistant at the Berkman Klein Center for Internet & Society Cyberlaw Clinic in Cambridge, MA, where she analyzed state and federal regulations and enforcement actions, regarding journalist rights, fourth amendment rights, cyberstalking, drone usage, and home surveillance technology. Additionally, she worked as a legal intern at the Data Privacy and Security Division of the Massachusetts Attorney General's Office, North Carolina Attorney General's Office, and a summer associate at a firm in Massachusetts.

Samuel Kane, Associate, WilmerHale

Samuel Kane focuses his practice on cybersecurity and privacy matters. In his current role, he assists companies in responding to government cybersecurity and data privacy investigations; aids companies' compliance efforts in relation to various state, federal, and international cybersecurity and data privacy legal frameworks; and supports companies' responses to cybersecurity incidents and data breaches. He is also a regular contributor to the WilmerHale Privacy and Cybersecurity Law Blog, where he writes primarily on state and federal privacy and cybersecurity law topics.

Prior to joining the firm, Mr. Kane clerked for the Honorable Paul V. Niemeyer of the US Court of Appeals for the Fourth Circuit. While pursuing his legal education, Mr. Kane was a summer associate at WilmerHale and served as a legal intern in the Department of Justice's Computer Crime and Intellectual Property Section.